REMARKS

1.   <u>Continuing Prosecution of the '146 Application</u>

The purpose of the present application is to continue prosecution of the application previously pending as serial no. 09/235,146 (the '146 application). The '146 application was unintentionally abandoned as a result of Applicants unintentionally failing to file a response to the previously-outstanding final Office Action dated April 22, 2002.

Although the '146 application has gone abandoned, the text of the '146 application was incorporated by reference in currently-pending application serial no. 09/236,366, which was filed on the same day as the '146 application and shares common inventors. The present application, which (other than the amendments to the claims and the priority recitation made herein) is textually identical to the '146 application, claims priority to the '366 application and back to the January 23, 1998 filing date of the provisional application no. 60/072,316 to which both the '366 and '146 applications claimed priority.

In view of the foregoing, Applicants view this application as continuing the substantive prosecution begun in the '146 application.

2.   <u>Response to the Final Office Action Issued in the '146 Application</u>

Applicants respectfully assert that the claims as pending patentably distinguish over the prior art applied in the final Office Action of the '146 application, which presented a rejection of each of the independent claims under §103 as purportedly being obvious over U.S. Patent No. 5,991,414 (Garay) in view of U.S. Patent No. 5,742,807 (Masinter). That rejection is respectfully traversed.

Initially, Applicants note that a number of amendments have been made to the claims to broaden and/or clarify them. None of these amendments was made to distinguish the claims over the prior art, as it is believed that the claims as previously pending were already distinguishable over the prior art. Furthermore, Applicants rely only upon the language of the independent claims themselves, as well as any arguments made in this paper for the purpose of distinguishing over the prior art of record. Applicants do not rely in any way upon any arguments previously presented during the prosecution of the '146 application. Therefore, the Examiner is respectfully

requested to examine the claims based only upon the language of the claims themselves, and any arguments made herein.

The final Office Action in the '146 application concedes that Garay fails to teach a number of limitations in each of the independent claims, but asserts that Masinter teaches one-way hashing of files and that it would have been obvious to one of ordinary skill in the art to include the Masinter file system in the system of Garay "in order to enhance the secure transmission of the distributed files in networking environment." (final Office Action, page 4). As discussed below, this assertion is entirely without support in the prior art of record, as nothing suggests that adding the file system of Masinter into the system of Garay would somehow enhance secure transmission of the files in the distributed Garay system. Thus, the Office Action fails to provide any motivation for the alleged combination, such that no prima facie case of obviousness was established. In addition, the final Office Action also fails to set forth a prima facie case of obviousness because it fails to provide any explanation of the nature of the system that it is alleged that one of skill in the art would have been motivated to arrive at based upon the teachings of Masinter and Garay, and no explanation is provided as to how this hypothetical system that allegedly would result from the combined teachings of these references would meet all of the limitations of each of the independent claims. In fact, as discussed below, each of the claims patentably distinguishes over any combination of Garay and Masinter.

A.   Garay

Garay is directed to a distributed system for storing and retrieving data. (See e.g., the title). Referring to Fig. 1, the distributed system (referred to as SSRI) includes a number of servers interconnected by a network. The user deposits and retrieves data by communicating with a single one of the servers, referred to as a gateway (GW) server. (col. 5, lines 35-37).

The protocol for depositing a file is shown in Fig. 3, and described at col. 10, line 17 – col. 11, line 53. The user transmits the file to the gateway, along with the user's signature, and retains a hash of the file for future use. (col. 10, lines 18-21). At 310, the gateway broadcasts the file to some of the other servers, which in turn (at 320) echo the file to the remaining servers such that every "correct" (i.e., functioning) server has a copy of the file (col. 10, lines 24-27 and col. 11, line 9).

722735.1

Once all of the servers have a copy of the file (col. 11, line 30), the system goes through a process referred to as "dispersal". The dispersal process requires only action or computation locally on each server, as the servers do not communicate during the dispersal process. (col. 11, line 30). As a result of the dispersal process, each of the servers will not store the entire portion of the file, but rather only the server's appropriate share of the file. (col. 11, lines 31-37). In addition to storing its own share of the file, each server also determines the hashes for the other pieces of the file and saves them as well. (col. 11, lines 31-37).

The retrieval process is shown in Figs. 5A-B and described beginning at col. 11, line 55. The user sends a request to the gateway to get the file back and includes some "information identifying the deposit" which is not further described. (col. 12, line 12). The gateway forwards the retrieval request to all of the servers (at 610 in Fig. 5A) and each server sends its share of the file back to the gateway along with the hashes of the other shares. (col. 12, lines 19-21). The gateway uses the hashes to determine which shares of the file that it receives are valid, and then reconstructs the file from the shares that are determined to be good (at 630 in Fig. A and described at col. 12, lines 21-25). The gateway then returns the file to the user at 640 (Fig. 5B).

B.   Masinter

Masinter is directed to an indexing system for a document management system as shown in Fig. 1. The document management system 10 includes three components, i.e., a document management index 12, a hash-to-hash location index 20 and a file system 28. (col. 4, lines 2-3). Masinter teaches that a hashing function can be used to establish a link between the document index and the actual storage locations of the documents in a file system. (col. 2, lines 15-17). Thus, a one-way hash function is used to process the document to create a hash, and then the hash is placed in the hash-to-hash location index that maps the hash to the physical address storage location. (col. 2, lines 20-25). In this way, the hash functions as an intermediate link between an attribute that is employed by a user of the system to access a document, and the actual physical address location for the document. (col. 2, lines 25-27).

722735.1

C.   The Alleged Motivation For Combining Masinter and Garay
      Is Entirely Without Support In The Prior Art of Record

The final Office Action in the '146 application alleges that one of ordinary skill in the art would have been motivated to use Masinter's file system in the system of Garay "to enhance the secure transmission of distributed files in networking environment." (Office Action, page 4). There is simply nothing in the prior art of record to suggest that the system of Garay is lacking in any respect in the security of the transmission of files in Garay's distributed network. In fact, the main thrust of Garay is directed to ensuring secure storage and retrieval of information. (see e.g., the title and col. 1, lines 6-10). Thus, there is nothing in the prior art of record to suggest deficiencies in the security of the Garay system that would have motivated one of skill in the art to modify it to increase security.

In addition, the system of Masinter is directed to providing a hash function that provides an intermediate link between an attribute used to access a file and the physical storage location for the file, and does not relate in any way to enhancing the security of transmission in a distributed file system. Thus, nothing in the prior art of record supports the assertion that one of skill in the art would have been motivated in any way by the teachings of Masinter to modify the system of Garay to increase the security thereof.

Finally, the disclosures of Garay and Masinter actually teach away from any combination. In this respect, Masinter is directed solely to performing a hashing function to create an index that provides an intermediate link between an attribute and a physical storage location. In the distributed system of Garay, the file is stored on each of the servers (Fig. 1), such that no indexing technique would be employed to determine which server stores a particular file, as it is distributed among all of the servers. Thus, the indexing technique employed by Masinter is simply not applicable to the distributed storage system of Garay.

D.   Each of the Independent Claims Patentably Distinguishes
      Over Any Combination Of Garay and Masinter

Even if one of skill in the art were motivated by Masinter to modify Garay in some respects, each of the independent claims patentably distinguishes over any combination. As discussed above, the final Office Action in the '146 application did not specify the nature of the

722735.1

system that one of ordinary skill in the art purportedly would have been led to based upon the combined teachings of Masinter and Garay. If the claims in the present application are rejected over such a combination, the Examiner is respectfully requested to describe the nature of the system configuration that one of ordinary skill in the art purportedly would have been led to based upon the teachings of Garay and Masinter, and to further explain how such a configuration would employ each of the limitations in the Applicants' claims.

1.   Claims 1-10 and 14-15

Independent claim 1 recites a number of steps that are not taught by either Garay or Masinter, and therefore are not taught by any purported combination of these two references.

Claim 1 is directed to a method that comprises acts of receiving, at a data repository, a broadcast cryptographic hash descriptor file identifier that identifies a digital asset; determining whether the identifier is known to the data repository, and when it is, adding the identifier to a list of desired identifiers. In addition, the method comprises acts of receiving, at the data repository, the digital asset identified by the broadcast identifier, generating a cryptographic hash file identifier from the received asset, and verifying that the generated identifier matches the broadcast identifier.

The distributed system of Garay works in a fundamentally different way. Initially, it is not an identifier for an asset (the type of asset described in Garay is a file) that is broadcast from the gateway server over the network to the other servers, but rather, it is the file itself that is broadcast. (see e.g., Fig. 3 at 310 "GW BROADCASTS FILE TO OTHER SERVERS"). Thus, each of the servers does not receive a broadcast cryptographic hash descriptor file identifier for a digital asset (e.g., the file) as recited in claim 1, but rather it receives the asset itself.

Claim 1 further requires that a determination be made as to whether the broadcast identifier is known to the data repository, and when it is not, adding the broadcast identifier to a list of broadcast identifiers. The Office Action in the '146 application asserted that the determining step was shown by Figs. 7A-B of Garay, which relates to a retrieval protocol (col. 4, lines 65-67). However, according to the retrieval protocol of Garay, when a retrieval request is forwarded to a server and identifies a file stored on the server, the server responds by returning to the gateway its share of the file (col. 12, lines 19-20). There is no disclosure that it adds the broadcast identifier to a list of desired identifiers as recited in claim 1.

722735.1

The Office Action in the '146 application concedes that Garay does not teach the steps of receiving, at the data repository, the digital asset; generating a cryptographic hash descriptor file identifier from the received asset; and verifying that the generated identifier matches the broadcast identifier. However, the Office Action asserts that Masinter teaches one way hashing of files and an "authentication process", citing the abstract and col. 3, lines 1-27. Applicants have reviewed the cited sections of Masinter, but no disclosure is present about verifying that a generated cryptographic hash descriptor file identifier matches a broadcast identifier. Thus, this feature recited in claim 1 also is clearly not taught by the prior art relied upon in rejecting the claim in the '146 application.

As should be appreciated from the foregoing, there are numerous limitations recited in claim 1 that are not taught or suggested by Masinter or Garay. Therefore, it is respectfully asserted that claim 1, as well as claims 2-10 and 14-15 that depend therefrom, patentably distinguishes over the prior art of record.

2.   Claim 11

Independent claim 11 is directed to a data repository to be coupled to a network. The data repository comprises an asset collector to: receive a broadcast cryptographic hash asset identifier, add the identifier to a list of desired identifiers, receive an asset identified by the identifier, and verify the identity of the received asset by generating a cryptographic hash asset identifier from the received asset and comparing it to the broadcast identifier. As should be appreciated from the foregoing, the prior art of record does not teach or suggest a data repository including such an asset collector. Therefore, it is respectfully asserted that claim 11 patentably distinguishes over the prior art of record.

3.   Claim 12

Independent claim 12 is directed to a method for selectively storing data in a data repository. The method comprises receiving, at the data repository, a broadcast cryptographic hash digital asset identifier, determining whether the identifier corresponds to an asset stored in the repository, adding the identifier to a list of desired identifiers when the broadcast identifier does not correspond to a received asset, and broadcasting the received asset stored in the repository when the identifier corresponds to a received asset stored in the repository.

722735.1

As should be appreciated from the foregoing, the prior art of record does not teach or suggest adding a broadcast cryptographic hash descriptor file identifier to a list of desired identifiers when it does not correspond to a received asset stored in a data repository. In this respect, Garay teaches a system wherein it is files (not cryptographic hash descriptor file identifiers) that are broadcast to the servers. Furthermore, Garay does not teaching adding an identifier to a list of desired identifiers when a broadcast identifier does not correspond to an asset stored in the data repository. Therefore, claim 12 patentably distinguishes over the prior art of record.
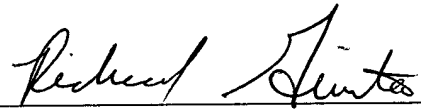
4.   Claim 13

Claim 13 is directed to a method of deleting a digital asset in a data repository that includes an asset list identifying the digital asset as being stored in the repository. The method comprises receiving, at the repository, a broadcast cryptographic hash descriptor file identifier; adding the identifier to a list of files to be deleted; comparing the identifier to a generated cryptographic hash asset identifier for the digital asset; and deleting the digital asset from the list when the broadcast identifier matches the generated asset identifier. The prior art of record simply does not teach or suggest a method of deleting a digital asset as recited in claim 13. In this respect, it is respectfully pointed out that the final Office Action in the '146 application did not even reference any portion of Garay or Masinter that was believed to support the deleting of an asset in any manner, let alone in the manner recited in claim 13. It is respectfully asserted that claim 13 patentably distinguishes over the prior art of record.

722735.1

CONCLUSION

In view of the foregoing amendments and remarks, this application is believed to be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes after this amendment that the application is not in condition for allowance, he is respectfully requested to contact the undersigned at the number listed below to discuss any outstanding issues relating to the allowability of the application.

Respectfully submitted,
Paul R. Carpentier et al., Applicants

By: _____

Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No. E00295.70192.US
Date: September 26, 2003
xNDDx

722735.1